



Regarding payments or other services the card may provide. The Examiner further cited col. 1, lines 10-25 and col. 2, lines 50-55 as teaching a mobile telephone handset, where a smart card is arranged to be inserted into the handset and an input interface for indicating a value to be loaded onto the smart card, the handset being arranged to generate a request message to load value onto the smart card. The cited passage discusses mobile phones, but not an arrangement for loading value onto a smart card. For at least these reasons, claim 1 is not anticipated by Heinonen.

**Claim 2** is dependent on claim 1, and for at least this reason is not anticipated by Heinonen.

**Regarding claim 5**, the Examiner cited col. 1, line 57-col. 2, line 14 and col. 10, lines 17-27 as teaching that the smart card is able to be removed from the handset to interface with a point-of-sale terminal. Although, col. 1, line 57-col. 2, line 14, teaches removable cards, col. 10, lines 17-27 teaches that the card connects to an electronic point of sale through the IR transmitter/receiver of the handset. Therefore, Heinonen does not teach that the smart card is removed from the handset to connect to a point-of-sale terminal, but that the card must be in the handset to connect to a point-of-sale device. In addition, claim 5 has the limitations of claim 1 discussed above. For at least these reasons, claim 5 is not anticipated by Heinonen.

**Claims 6 and 7** are dependent on claim 5, and for at least for this reason are not anticipated by Heinonen.

**Regarding claim 12**, the Examiner stated col. 1, lines 49-56, col. 1, lines 38-42, and col. 2, lines 22-42 teaches loading value over a telecommunications network onto a smart card. Col. 1, lines 49-56, discloses disadvantages of payment cards on which money value is loaded, and that to load value on such cards requires loading the value at a sales outlet that offers a loading service. Col. 1, lines 38-42, discloses that smart cards may be used for payments. Col. 2, lines 22-42 discloses that various application modules may be used on a telephone smart card. None of these passages discloses loading value onto a smart card over a telecommunications network. In addition, the Examiner stated that the receiving a response message which includes the authentication response certificate and the validating said authentication response certificates are disclosed by col. 3, lines 31-36 and 44-56 of Heinonen. Nothing in the cited passages of Heinonen discloses validating an authentication response certificate. For at least these reasons, claim 12 is not anticipated by Heinonen.

**Claims 13 and 14** are dependent on claim 12, and for at least this reason are not anticipated by Heinonen.

**Claims 16-18** have been cancelled.

The Examiner rejected **claims 8 and 15 under 35 USC § 103** as being unpatentable over Heinonen. The Examiner stated that Heinonen does not explicitly disclose that, in response to a successful load, the handset is arranged to generate a transaction certificate to be used for irrepudiation. The Examiner took Official Notice that it is old and well known in the payment arts that, in response to a successful load, the handset is arranged to generate a transaction certificate to be used for irrepudiation. The applicants traverse such an assertion and respectfully request that the Examiner provide a cited reference to support his position of it being known to use a handset to generate a transaction certificate used for irrepudiation. The Examiner has failed to respond to applicants' previous requests for such references. For at least these reasons, claims 8 and 15 are not made obvious by Heinonen.

The Examiner rejected **claims 4 and 9-11 under 35 U.S.C. § 103** as being unpatentable over Heinonen and further in view of Jonstromer (WO 96/32700). **Regarding claim 4**, the Examiner stated that Heinonen discloses a smart card loading system as recited in claim 1, but does not explicitly disclose that the authentication computer authenticates the smart card using a first cryptographic signature and generates a second cryptographic signature to authenticate a load response, whereby the transaction is secured. The Examiner further stated that Jonstromer discloses such steps on page 1, line 24, to page 2, line 8, and on page 8, lines 25-32, and on page 13, line 31, to page 14, line 9, and on page 16, line 13, to page 17, line 22. The Examiner said it would be obvious to authenticate the smart card using the first cryptographic signature and generate a second cryptographic signature to authenticate a load response for the purpose of increasing system security. Claim 4 is dependent on claim 1 and for at least this reason is not made obvious by Heinonen in view of Jonstromer.

**Claim 9** further recites removing the smart card from the handset and placing the removed smart card in contact with a point-of-sale terminal to provide a contact interface with said point-of-sale terminal, and using the point-of-sale terminal to debit said smart card to perform a purchase. Both Heinonen and Jonstromer teach away from this limitation. Instead of placing the smart card loaded by a mobile handset in physical contact with a point-of-sale terminal, Heinonen and Jonstromer both teach using the telecommunications network or IR or some other remote communication. The Examiner cites col. 10, lines 18-27 of Heinonen for teaching placing the smart card in contact with the point-of-sale terminal. This passage teaches that such contact is made by an IR data transfer. Such a transfer is made when the card is in the handset. Therefore, this passage does not teach placing the removed smart card in contact with

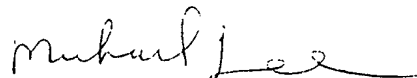
the point-of-sale terminal, as recited in claim 9. For at least these reasons, claim 9 is not made obvious by Heinonen in view of Jonstromer.

**Claims 10 and 11** are dependent on claim 9, and for this reason are not made obvious by Heinonen in view of Jonstromer.

The Examiner rejected **claim 3 under 35 U.S.C. § 103** as being unpatentable over Heinonen in view of Lawlor et al. The Examiner stated that Heinonen discloses a smart card loading system as recited in claim 2, but does not explicitly disclose the card reader is a Europay-Mastercard-Visa type of card reader, but that Lawlor discloses such as a step in a system which includes handset, smart card, subscriber identification, and POS (col. 41, lines 1-30) and that it would have been obvious to include that step in the Heinonen system to increase the use of the system. Col. 41, lines 1-30, does not disclose a Europay-Mastercard-Visa type of card reader. The applicants did not see any mention of a Europay-Mastercard-Visa type card reader or any other card reader in the cited passage. For at least these reasons, claim 3 is not made obvious by Heinonen in view of Lawlor et al.

Applicants believe that all pending claims, as amended, are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at telephone number (831) 655-2300.

Respectfully submitted,  
BEYER WEAVER & THOMAS, LLP



Michael Lee  
Reg. No. 31,846

P.O. Box 778  
Berkeley, CA 94704-0778  
(510) 843-6200